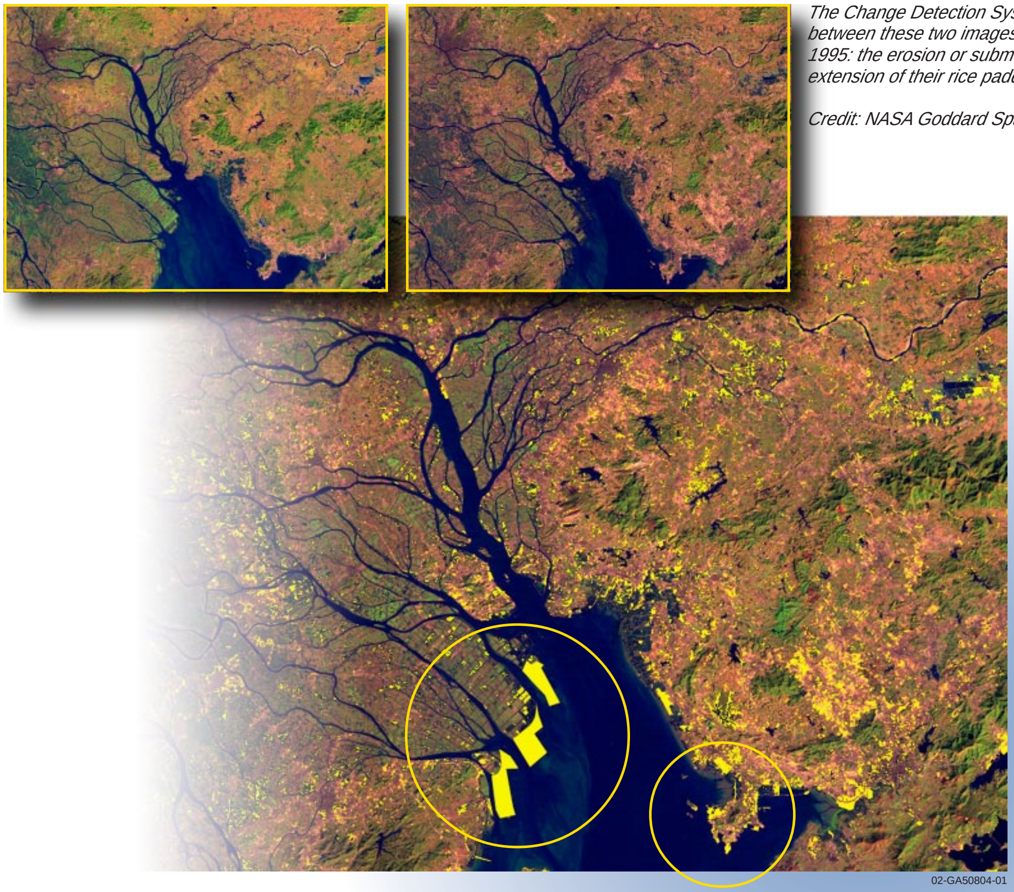
NEED TO KNOW

a national security newsletter

Volume 3, Number 4 August 2003

Suspicious Signs: Computer program exposes invisible changes.

Contributed by Nicole Stricker



The Change Detection System shows two significant changes between these two images of China's Pearl River taken in 1988 and 1995: the erosion or submersion of a peninsula and the farmers' extension of their rice paddies out into the river.

Credit: NASA Goddard Space Flight Center.

02-GA50804-01

From home security to homeland security, things just got a lot tougher for bad guys hoping to go undetected.

Telltale signs of mischief are often minuscule changes that are nearly invisible to the eye, even when comparing before and after images. But such signs become clear as day with the help of the Change Detection System developed by scientists at the INEEL. The computer program complements the natural power of the human visual system, deftly bypassing hurdles that can complicate comparison of images. The program's versatility makes it attractive to everyone from security guards to working parents, field researchers to physicians.

Be they photos of forged and authentic documents or container seals before and after tampering, side-by-side comparisons can reveal prominent differences. But subtle changes are often impossible to spot in similar pictures. Even computers struggle with the task. While they can scrutinize every pixel in a digital photo, image comparison programs often become bogged down by trivial differences in camera angles or lighting.

In the past, the best technology available for comparing digital images has been a technique known as flip-flop. Rapid computerized alternation, or flip-flopping, between two similar digital images creates an animation effect—identical

See **CDS**, page 2

IDAHO NATIONAL ENGINEERING AND ENVIRONMENTAL LABORATORY

INEEL

Home of Science
and Engineering Solutions

The CDS program developed by the INEEL's Greg Lancaster, James Litton Jones and Gordon Lassahn combines the strengths of rote computer analysis with the powerful human reflex elicited by the flip-flop comparison technique.

CDS *(continued from page 1)*

elements seem stationary while differences appear as movement. The approach capitalizes on the visual reflex that draws our eyes toward motion.

But the flip-flop method requires that both pictures be shot from the exact same position using a mounted camera. If the images aren't perfectly aligned, the whole picture moves during flip-flopping, drawing the eye only toward the differences in camera angle. Since the use of stationary cameras is often impractical, flip-flop comparisons are rarely possible.

Now, the CDS program developed by the INEEL's Greg Lancaster, James Litton Jones and Gordon Lassahn combines the strengths of rote computer analysis with the powerful human reflex elicited by the flip-flop technique. The CDS software aligns digital images to within a fraction of a pixel, enabling flip-flop analysis of images taken with a hand-held digital camera. The software compensates for modest differences in camera angle, height, zoom or other distractions that previously confounded flip-flop comparisons.

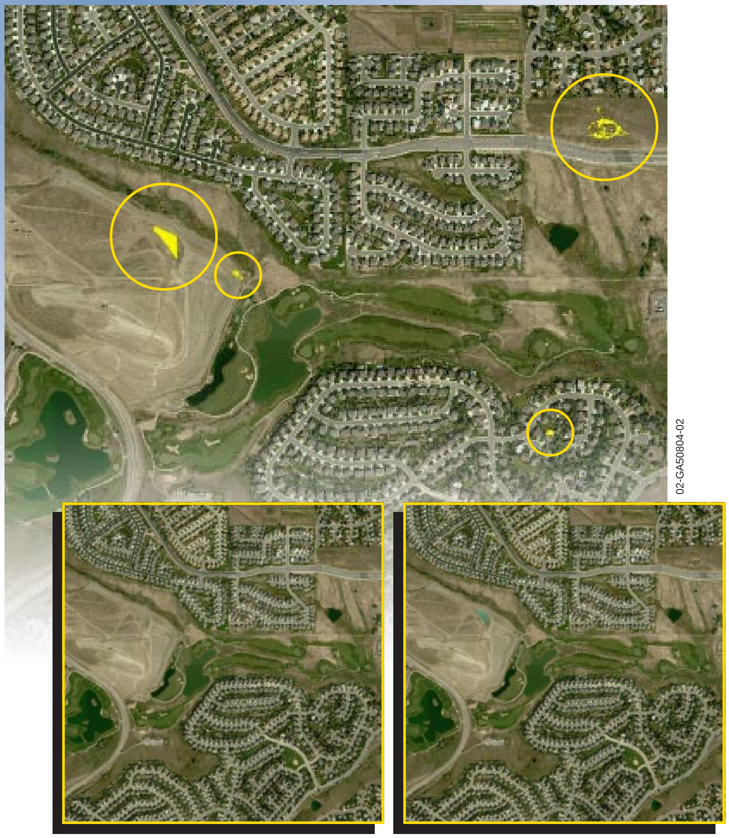
Flipping between two seemingly identical images aligned by CDS can reveal once imperceptible differences—tiny defects in container locks betray tampering, infinitesimal imperfections expose counterfeit bills, and footprints appear in a gravel road. The CDS technology was developed by the National Security Division of the INEEL through funding from the DOE Applied Technology Program, and initiated with the help of a Laboratory Directed Research and Development investment.

Yet potential applications for CDS extend far beyond the security realm. Proponents of the software are adapting its use to applications ranging from forensics to geology to medicine. Using the CDS program, surveillance officers could detect whether doors have been opened or cars have been moved. Forensic scientists could analyze CDS aligned images of tire or shoe prints. Physicians may one day compare yearly medical scans to detect early stages of disease. Even homeowners could use CDS to divulge whether drawers or rooms have been disturbed. And field researchers could track environmental changes on a day-to-day basis.

"We can now monitor erosion not boulder by boulder, but grain by grain," said Jerry Harbour, an INEEL consulting scientist exploring the cognitive process behind change detection.

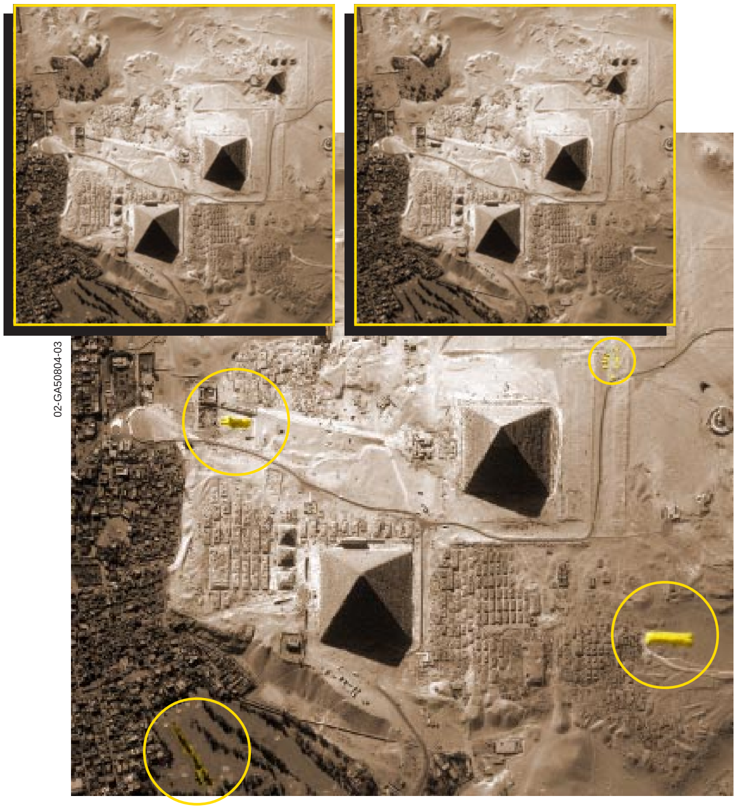
Now that the development of CDS has made the flip-flop technique a practical tool, Harbour and his team in Human/Intelligent Systems are studying how the approach measures up to other common photo analysis techniques. The researchers record how quickly and accurately untrained

Most people can spot the lake and building missing from the left photo, but the Change Detection System reveals that a swimming pool and a dirt track are also absent. (credit: Space Imaging®, Digital Airborne Imaging System)



volunteers can pick out differences between CDS-aligned photos. Volunteers are assigned one of three common comparison methods: side-by-side, flip-flop, or flicker—a variation of flip-flop where alternating images are separated by 0.15 seconds of gray screen (roughly the duration of a long blink). The subjects are asked to rapidly identify differences between 20 pairs of photos. Harbour and his colleagues Heather Hunting, Heather Medema and Jeffery Joe then compare speed and accuracy between subjects using different techniques.

The Change Detection System shows that the sphinx, a mountain, a line of trees, and several large vehicles are missing from the left image. (credit: Space Imaging®, Ikonos satellite)



Harbour discovered that the flip-flop comparison method drastically improves the efficiency of change detection. Side-by-side comparisons took up to four times longer than other strategies and compromised accuracy, which fell as low as 55 percent. The flicker approach was slightly faster, but accuracy dropped to nearly 30 percent in some cases. Yet people using the flip-flop method were consistently more than 90 percent accurate and spotted differences two to ten times faster than subjects using the other comparison techniques. Next, Harbour hopes to test the CDS technology, which uses the flip-flop approach, with trained photo analysts.

“These are people who are paid to search through side-by-side images looking for differences, but it takes them all day to pick out changes akin to the ones our volunteers find in less than a minute,” Harbour explains. “Imagine what this could do for their job efficiency.”

The CDS alignment process takes only seconds and the software is simple enough to be operated by a 10-year-old child. What’s more, the program is small, only 350 KB, and can operate on a standard PC, laptop, or even a handheld computer. Retail versions of CDS will likely sell at prices comparable to ordinary business software.

The CDS program is so quick, easy and affordable that it now boasts a spot among the 100 most technologically significant products introduced in the past year. R&D Magazine editors notified the winners in July and will feature the winning products in the magazine’s September issue.

One medical technology firm is already looking to license the program. The medical applications first became clear to lead researcher Lancaster as he grappled with a brain tumor while working on the CDS project. After doctors removed the growth, they monitored Lancaster’s brain with twice yearly MRI scans to make sure the tumor didn’t return. As his physicians squinted at the images, searching for the tiniest change, Lancaster worried they might miss something.

“They just stare at them to try to find differences,” said Lancaster. “I said, ‘Man, that’s so archaic,’” Lancaster decided to test whether CDS improved his doctors’ powers of perception.

“I took an image, altered it ever so slightly, brought in both pictures and said, ‘Can you see a difference?’ They looked at the two images and admitted, ‘Well, no,’” Lancaster said. “But with the flip-flop method, it really pops out. They said, ‘Wow! What a tool!’”

Greg Lancaster
Gdl4@inel.gov

Greg Lancaster studies a pair of MRI images. CDS is also being considered for use in the medical community, where it could quickly spot tumors and other anomalies.

INEEL Cyber Security – Aggressive Defense Against an Unseen Enemy

Diehard science fiction fans know that writer William Gibson brought the word cyber to life in his 1984 novel *Neuromancer*. He coined cyberspace to refer to an electronic or virtual reality. Today, the meaning of the word has evolved to a synonym for electronics or computers. Cyber, however, still evokes the image of data invisibly racing to destinations around and beyond the globe, while the word computer recalls the familiar display and hard drive found in almost every home and office. Cyber security protects computers, systems and networks from enemy attacks. INEEL's cyber security is both an art and a science.

The INEEL Web site, like many .gov locations, is a prime target for hackers. The site is bombarded with thousands of scans each day – over 90,000 on average weekly. The perpetrators may be trying to weasel their way into the network out of curiosity or with malicious intent. They may be cold professional criminals looking for vulnerabilities to exploit or sell, or they may be citizens of a hostile nation, patiently gathering information, byte by byte. Rob Hoffman leads a team of equally professional computer whizzes whose job it is to keep them out. And they take it very personally.

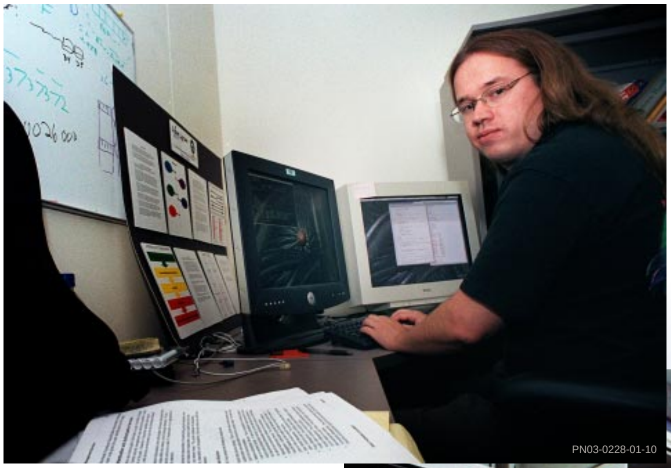
The handpicked team was assembled several years ago after a hacker got in. The individual 'touched a box,' to use computer lingo – by reaching a server with the potential to modify its contents. Disaster was diverted and no damage was done, but the aftertaste remained. As good as INEEL's computer security had been, it now had to be even better.

"Cyber Security focuses on assisting the programs in accomplishing their missions in a secure fashion," said Hoffman, summarizing the organization's goal. "It's a dynamic process. Security should never inhibit success, but the integrity of the enterprise is paramount."

The first daunting task facing the team was identifying the existing potential avenues of risk. They put together a spreadsheet for the external servers. It listed thousands of vulnerabilities. The goal was to clean up the servers in six months. They did it in three.

Red Team/Blue Team

But every Wednesday like clockwork, vicious attacks still flood INEEL computers. This time around, however, the bad guys are the good guys. The Cyber Security staff takes turns attacking and defending the system. For example, someone may take the lead on launching a particularly nasty exploit and the rest of the group defends against it. All of this, of course, is conducted on a closed network, but the results benefit every computer user at the laboratory. And the game playing keeps the staff sharp and prepares them to deal with the reality of cyber defense.



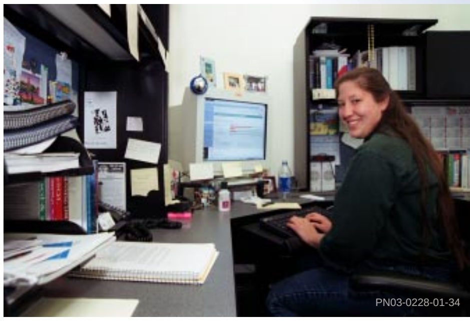
Jason Larsen (above) wrote the genesis of Hogwash intrusion detection software while still in college.

"My job, the job of every team leader or manager, is to keep staff challenged, give them the tools and training to do their work, and remove obstacles," said Hoffman. "The red team/blue team efforts really challenge our group to enter the mindset of the hacker."

Collaborative Excellence

The Cyber Security organization supports both operational activities and programmatic customers and is collocated within Information Technologies and the National Security Division. The rationale for the organization's support to the Division is clear enough when you consider that the laboratory is a national asset that must be protected. But the Cyber Security wizards do more than guard our gates; they conjure up some mean magic for federal agencies and military groups wanting to protect their cyber treasures.

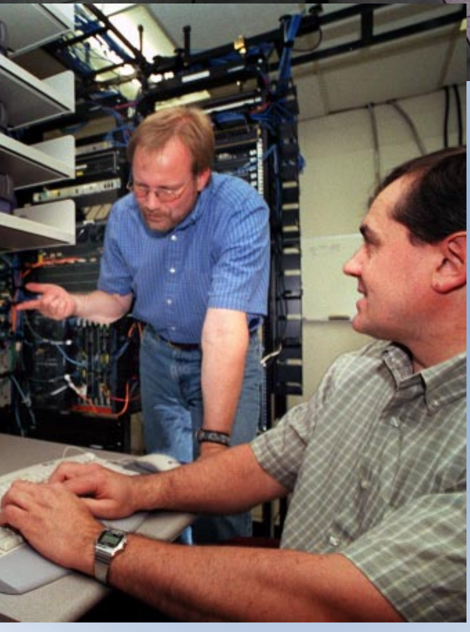
Instead of causing conflicts between fulfilling the routine needs of the



The Cyber Security staff, such as Liz Faultersack (above), takes turns attacking and defending the system. For example, someone may take the lead on launching a particularly nasty exploit and the rest of the group defends against it.

PN03-0273-01-35

The laboratory is building a specialized cyber test bed (above) to support customers and projects that must be kept separated from even the closed networks due to the proprietary nature of the work or at the request of the agency.



Rob Hoffman (working with Kevin Barnes at left) leads a team of handpicked computer whizzes whose job it is to keep hackers out of the INEEL's computer systems.

laboratory and responding to the sometimes-exotic requests of clients, the two roles of Cyber Security create a symbiotic relationship between the functions that enhances them both.

For example, Hoffman's team doesn't just use intrusion detection software, team members write their own. They apply this expertise first to INEEL networks, where their tool is sensitive enough to pick up the slow scans than run below the radar of most commercial detection programs. Intrusion detection, however, is more than just a software program. According to Hoffman, it takes a certain mindset, an intuitive feel to detect the traffic patterns within all of the data. The team has this touch.

So when the Department of Defense's Defense Information Systems Agency looks for intrusion detection experts, they look to the INEEL. For the last several years, Cyber Security staff has worked to integrate custom Snort plug-ins into DoD's new intrusion detection program, agencywide.

This synergy works both ways according to Kevin Barnes, a Cyber Security team member who primarily focuses on supporting external customers. Barnes has access to the INEEL network that allows him to build and test tools that keep his customer and the laboratory a step ahead of the competition – not other laboratories, but the hackers.

The collaboration between operations and programs isn't just a good idea; it is essential.

The laboratory's key mission area within National Security is critical infrastructure assurance. The Division operates complex SCADA (Supervisory Control and Data Acquisition) and Wireless test beds with government and commercial partners (see Need to Know, January 2003 and April 2003). The test beds are used to identify vulnerabilities, and develop and test solutions. Cyber security is an integral component since SCADA and wireless communications systems are especially vulnerable to malicious electronic attacks.

The laboratory is building a specialized cyber test bed to support customers and projects that must be kept separated from even the closed networks due to the proprietary nature of the work or at the request of the agency.

"Zero-Day" Exploits

Outside of the black hat or hacker community, few have heard or recognize the phrase "zero day," which refers to that nebulous time between the discovery of a vulnerability in a software program and the launching of the patch to fix it, when "Day 1" begins. Zero-day exploits can cause irreparable harm, destroying data, introducing viruses and stealing information.

The Cyber Security team works hard to remain a step ahead of the hackers to minimize zero-day exploits. When the NIMDA virus infected the nation's computer systems, it contained a virulent strain designed to attack .gov domains. The team reverse-engineered the virus to develop a defense and met with the commercial anti-virus software provider to create the solution. The INEEL network was safe before the patch hit the streets.

Another way they stay ahead of the hackers is to infiltrate their lines, officially. Hoffman and colleague Jason Larsen have attended international hacker conferences and rubbed elbows with the top 20 to 25 "ubergeeks" in the world, most younger than 30 years old. A common trait among this elite group is an early curiosity about how things work, in this case, infrastructure protocols and low-level code.

Larsen could be considered a card-carrying member of these privileged few, having published his first code at age 13. And while still in college, he wrote the genesis of the Hogwash intrusion detection software, and made it available on the Internet as an open source project. The Web site for Hogwash describes how to set up a honeypot, which is a network configuration that allows a user to observe attackers in a safe environment while protecting their own production server. The source code for establishing a honeypot is followed by some simple instructions that epitomize not just Larsen's attitude but many of those at the INEEL who go into electronic combat daily. "That's about all there is to it. Have fun."

Rob Hoffman
hoffrw@inel.gov

FireView – Breaching a Firewall…Legally

Contributed by Mark Montie

Sometimes the National Security Division — normally recognized for creating solutions to counter threats against the nation — focuses on solving problems a little closer to home. Such is the case with FireView, a system that allows engineers to share sensitive data for non-engineering purposes inexpensively and securely over the Internet.

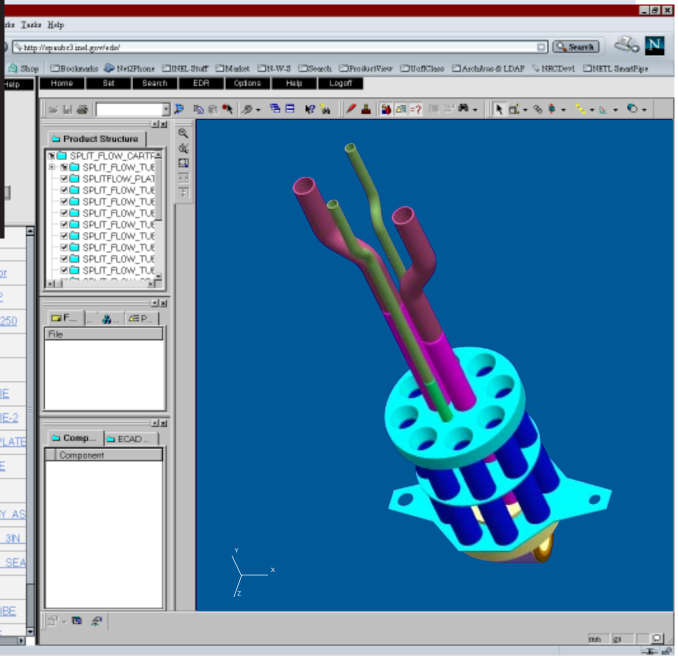
The Internet has become the medium of choice for conveying information quickly. Cost, bandwidth and security issues, however, have been limiting factors in using the Internet to send large amounts of sensitive engineering data.

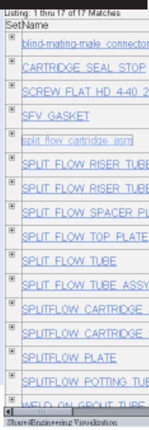
Often engineers need to send engineering files outside a firewall, a company's gateway machine with special security precautions used to limit access to a computer network. This creates security issues when commercially sensitive data is being shared through the non-secure environment of the Internet. Also, common engineering files like 3-D images are often so large that they put strain on Internet connections transferring them.

PN03-0227-01-03

"We need to share engineering data with people outside the company, but they don't always need full blown engineering capabilities, they just may want to look at a design or get a picture."

Dan Kurkowski





Listing: 1 thru 17 of 17 Matches

SetName

blind-mating-male connector
CARTRIDGE SEAL STOP
SCREW FLAT HD 4-40 250
SFV GASKET
split flow cartridge asm
SPLIT FLOW RISER TUBE
SPLIT FLOW RISER TUBE-2
SPLIT FLOW SPACER PLATE
SPLIT FLOW TOP PLATE
SPLIT FLOW TUBE
SPLIT FLOW TUBE ASSY AS
SPLITFLOW CARTRIDGE 3IN
SPLITFLOW CARTRIDGE SEA
SPLITFLOW PLATE
SPLITFLOW POTTING TUBE
WELD ON GROUT TUBE

Shared Engineering Visualization

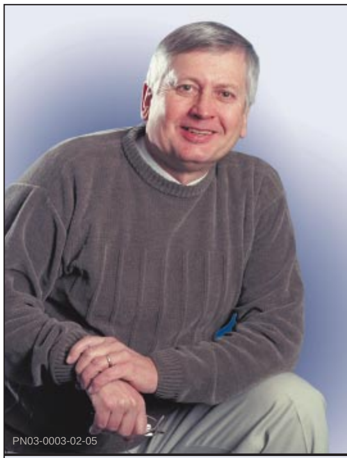
03-GA50804-04

For years, software has been available to send engineering data over the Internet. It is very costly, and primarily serves those with top-of-the-line engineering software applications. Dan Kurkowski, a technical specialist in National Security's Integrated Defense Systems, and the creator of FireView, said many organizations would benefit from a smaller-scale solution. "We need to share engineering data with people outside the company, but they don't always need full blown engineering capabilities, they just may want to look at a

Almost Prime Time

National Security's Mike Occhionero and Kevin Young have been busy sharing their passion for what they do with the next generation of researchers. Occhionero and Young appeared on Idaho Public Television's "Dialogue for Kids" to show off a variety of INEEL-developed intelligence-gathering technologies, and to answer dozens of questions from students across the state. With support and materials from the laboratory, Idaho Public Television also launched a companion interactive Web site.

PN03-0186-02-20



State of the Division

Laurin Dodd,
Associate Laboratory Director, National Security

It is no coincidence that all of the articles in this issue of Need to Know address computers and security. Wired or wireless, military or civilian, we are inextricably connected to the computer. The National Security Division is dedicated to protecting our citizens and the assets of the nation – physical or electronic – and we do this through some of the most innovative computer-based technologies and with some of the brightest people.

R&D Magazine recognized this, too, when it gave an R&D 100 award to National Security's Greg Lancaster and James Jones who, along with Gordon Lassahn (ret.), developed the Change Detection System. The CDS software precisely aligns images from a handheld digital camera and highlights differences that would otherwise be virtually invisible to the human eye, making minuscule changes seem to leap out of the images. The CDS technology is easy to use and has applications ranging from national and homeland security to medical imaging and basic research. I join co-workers throughout the INEEL in congratulating Greg, James and Gordon for their achievement.

Cyber warfare rages daily and the Division's staff is on the front line, not only protecting the laboratory's wealth of data, but also that of our national security clients. These computer masterminds speak a new language, written, for the most part, in just one generation. They're working hard to keep our defenses impregnable.

But when we do want to share our knowledge over the vulnerable Web, we have engineers designing safe, inexpensive methods to do so, and we talk about that in this issue.

Over the last several issues of this newsletter, we've spoken about our Critical Infrastructure Assurance program and the SCADA and Wireless test beds that we use to design and test solutions for system vulnerabilities. Computers and security are at the heart of many of the vulnerabilities. We are fortunate that here at the INEEL, we have the people and the tools to create the solutions.

design or get a picture," Kurkowski said.

Kurkowski and his engineering counterparts – Brian Raivo, Bryan Spaulding and Kent Warren – developed the system by integrating state-of-the-art commercial data management and visualization technology with homegrown software and methods designed to comply with the strictest Internet security regulations in the DOE system, namely those at the INEEL. The system was designed with 3-D images in mind, but it is applicable to all types of data, including graphics, text and complex design data. Kurkowski's expertise comes from a background of building vast integration systems like the Joint Logistic Systems Command, a system for integrating logistics from all branches of the military.

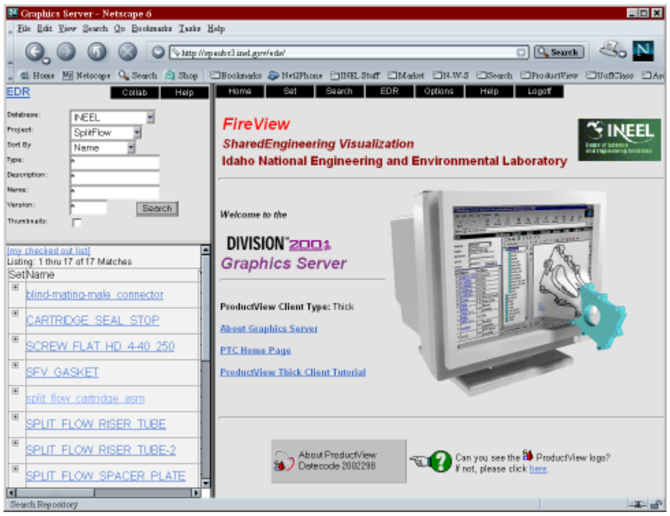
With FireView, INEEL engineers can design projects within the lab, where employees and technology resources are close at hand, securely behind its firewall. Then, in real time, they can share their data with clients on demand. FireView is believed to be the first system developed with this purpose in mind.

"We're trying to get a low-end product, not to do engineering worldwide, but to share the engineering we've done with people, inexpensively," Kurkowski said.

The system offers customers varying levels of functionality for associated costs. Customers could get a simple 3-D image for free. Or, at the high end, they could go online and make comments on a drawing without actually manipulating the originating secure file for a fraction of the cost of expensive engineering software.

FireView is currently in the demonstration phase, but

03-GA50804-05


Graphics Server - Netscape 6
File Edit View Search Go Bookmarks Tasks Help
Search
Home My Netscape Search Shop Bookmarks Net2Phone INEL Stuff Market N-W-S Search ProductView UofClass
EDR
Collab
Help
Home
Set
Search
EDR
Options
Help
Logoff
INEEL
Search
About ProductView Datecode 2002298

http://rpaubc3.inel.gov/edr/

Database: INEEL
Project: SplitFlow
Sort By: Name
Type: *
Description: *
Name: *
Version: *
Thumbnails: □

[my checked out list]
Listing: 1 thru 17 of 17 Matches

Set	Name
⊞	blind-mating-male_connector
⊞	CARTRIDGE_SEAL_STOP
⊞	SCREW_FLAT_HD_4-40_250
⊞	SFV_GASKET
⊞	split_flow_cartridge_asm
⊞	SPLIT_FLOW_RISER_TUBE
⊞	SPLIT_FLOW_RISER_TUBE-2
⊞	SPLIT_FLOW_SPACER_PLATE

FireView
SharedEngineering Visualization
Idaho National Engineering and Environmental Laboratory

Welcome to the
DIVISION™2001
Graphics Server

ProductView Client Type: Thick
About Graphics Server
PTC Home Page
ProductView Thick Client Tutorial

Can you see the ProductView logo? If not, please click here.

Search Repository

With FireView, INEEL engineers can design projects securely behind the lab's firewall. Then, in real time, they can share their data with clients on demand.

while, developing the system to serve INEEL's engineering clients remains a priority.

Kurkowski said he is prepared to move onward as customer interest in the system builds. The INEEL is exploring licensing FireView to other engineering labs that use similar 3-D imaging software. Meanwhile, developing the system to serve INEEL's engineering clients remains a priority.

Dan Kurkowski
djk@inel.gov

Partnership for Protection

Contributed by Bonnie Hong

The INEEL is taking an active role in a new chapter of an infrastructure security organization, InfraGard of the Wasatch.

InfraGard is a cooperative effort involving the exchange of information among the owners and operators of information systems, the business community, academic institutions and other government agencies. InfraGard was formed as part of the federal government's effort to protect the nation's eight infrastructures critical to the United States' economic and national security: Banking and Finance, Emergency Services, Government Operations, Transportation, Electrical Energy, Gas and Oil Storage and Delivery, Telecommunications, and Water Supply Systems.

InfraGard is a local, regional and national "grass-roots" effort to respond to the need for cooperation and collaboration in countering the threat to our infrastructures.

The INEEL is contributing and supporting the organization of a new chapter – InfraGard of the Wasatch – in conjunction with the cyber department in the regional Federal Bureau of Investigation office in Salt Lake City. The InfraGard of the Wasatch chapter is incorporated under the InfraGard of the Intermountain West region that covers Idaho, Utah and Montana.

The chapter membership consists of private-sector members and an FBI field representative. The membership sets up its own board of directors to govern and share information with each other and with other InfraGard chapters.

Members are linked to each other and to the FBI by the Bureau's secure "alert network." Companies can anonymously report incidents to all other members without fear of publicizing their vulnerability. The FBI provides encryption software to protect information exchange among members. The National Infrastructure Protection Center (NIPC) will use data gathered from different InfraGard chapters to compile reports on nationwide security trends. As the security risk grows, the InfraGard program is becoming the FBI's frontline of defense.

InfraGard of the Wasatch initially consisted of computer infrastructure-oriented members. However, with the Winter Olympics in Salt Lake City and the current world events, appeal has spread to all branches of law enforcement, government, academia, private industry, and many first responders.

InfraGard is a cooperative effort involving the exchange of information among the owners and operators of information systems, the business community, academic institutions and other government agencies.

Elected officers for 2003 are Bonnie Hong (INEEL), president; Dave Fletcher (state of Utah, Department of Administrative Services), vice president; and Ken Freimuth (ATK Thiokol), secretary. The FBI representative is Cheney Eng-Tow (FBI, SLC).

The purpose and primary objective of the InfraGard of the Intermountain West chapter is to provide forums for the exchange of information between infrastructure owners and operators and others concerned with the protection of the infrastructure. The goal of InfraGard is to enable the flow of information so that the owners and operators of infrastructure assets can better protect themselves, and the United States government can better discharge its law enforcement and national security responsibilities.

As a member of InfraGard, there are multiple benefits:

- Prompt threat warnings from the FBI and InfraGard members
- Education and training on cyber and physical security topics
- Opportunity to interact and share information with others from law enforcement, academia, private industry and other government agencies
- Discounts on books, training (SANS, MIS Training Institute, etc.) and conferences

For more information on InfraGard, go to www.infragard.net.

NEED TO KNOW is a publication of the National Security Division of the Idaho National Engineering and Environmental Laboratory. The INEEL is a science-based, applied engineering national laboratory dedicated to supporting the U.S. Department of Energy's missions in environment, energy, science and national security. The INEEL is operated for the DOE by Bechtel BWXT Idaho, LLC. Requests for additional copies, story ideas or questions should be directed to the editor at (208) 526-1058, kzc@inel.gov. This is printed on recycled paper.

Editor .... Kathy Gatens
Graphic artist .... David Combs
Photographers .. Mike Crane, Chris Morgan, Ron Paarmann
Copy editing ...... Rick Bolton
Research .... Steve Paschke

Visit our national security website at:
www.inel.gov/nationalsecurity

NEED TO KNOW